UNTIED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

BRADY COHEN, individually and on behalf of others similarly situated, Plaintiff, - v - CASPER SLEEP, INC. and NAVISTONE, INC., Defendants.	Case No. 1:17-CV-09325 (WHP)

DEFENDANT NAVISTONE, INC.'S MEMORANDUM IN SUPPORT OF ITS MOTION TO DISMISS

MENAKER & HERRMANN LLP
10 East 40th Street
New York, New York 10016
(212) 545-1900

BRANN & ISAACSON
184 Main Street, P.O. 3070
Lewiston, Maine 04243-3070
(207) 786-3566

Attorneys for Defendant NaviStone, Inc

March 1, 2018

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes and Rules

Other Authorities

Defendant NaviStone, Inc. ("NaviStone") respectfully submits this memorandum in support of its motion pursuant to Fed. R. Civ. P 12(b)(6) and 28 U.S.C. § 1367(c) to dismiss the Amended Complaints in three lawsuits brought by Plaintiff Brady Cohen ("Cohen") against NaviStone and its online retailer clients (the "Retailers"). As directed by the Court at the February 23 case management conference, this memorandum is addressed to all three cases. Other than the caption, the copies filed in each case are identical.

SUMMARY OF ARGUMENT

Cohen seeks relief against NaviStone and the Retailers under two federal statutes that do not apply. Congress did not enact the Wiretap Act, 18 U.S.C. § 2510, *et seq.* (the "Wiretap Act") to create liability for a retailer sharing communications from visitors to its website with its marketing service providers. Nor does the Stored Communications Act, 18 U.S.C. § 2701, *et seq.* (the "SCA"), apply to information stored on a user's own computer or other device. Cohen has also added state law claims under GBL §§ 349 and 350. These should be dismissed for failure to state a claim or in the Court's discretion under 28 U.S.C. § 1367(c).

The Wiretap Act. The Wiretap Act requires intervention by an unauthorized person into a communication between other parties. Cohen's allegations show that NaviStone has no liability under the Wiretap Act (Counts I through V) because (1) it was a party to the alleged communications; (2) there was no unlawful interception; (3) it had the prior consent of the Retailers (which are themselves parties to the communications) for all of the activities he describes; and (4) there is no private right of action for possession, marketing, and sale of interception devices.

The Stored Communications Act. Cohen's SCA should be dismissed because a website visitor's computer or other device is not "a facility through which an electronic

information service is provided." 18 U.S.C. § 2701(a).

State Law Claims. Cohen has added state-law "deceptive acts and practices " and "false advertising" claims under §§ 349 and 350 of the New York General Business Law. These, however, cannot survive either in tandem with the federal claims or as stand-alone claims because neither cognizable injury nor the requisite element of deception is alleged. In any event, if the federal claims are dismissed, the Court in its discretion should dismiss the state-law claims under 28 U.S.C. § 1367(c).

Accordingly, NaviStone respectfully asks the Court to dismiss these cases with prejudice and without further leave to amend.

ALLEGATIONS IN THE AMENDED COMPLAINTS

NaviStone assumes, as it must, that the factual allegations in the Amended Complaint[1] ("Amend. Compl.") are true, but solely for purposes of this motion. *DigitAlb, Sh.a v. Setplex, LLC*, No. 17-CV-4102, 2018 WL 377381, at *2 (S.D.N.Y. Jan. 11, 2018).

A. The Plaintiff

Plaintiff Cohen is a citizen of New York who claims standing to bring this lawsuit because, on "several occasions" during the prior six months, he "visited" the Retailers' websites (the "Retailer Websites") using an Android device, but made no purchases (Am. Compl. ¶¶ 2, 4). On these occasions, Cohen alleges that, while he "browsed" the Retailer Websites, his "keystrokes, mouse clicks and other electronic communications" were "captured" and redirected by the Retailers to NaviStone "in real time" and that his Android device was also "scanned" for

[1]While Cohen's three Amended Complaints involve different retailer defendants and have slight variations in paragraph numbering, they assert the same causes of action based upon materially identical factual allegations. For ease of reference, NaviStone will cite to the first filed case, against NaviStone and Casper Sleep, Inc., in its references to the Amended Complaint ("Amend. Compl.").

certain files (*id.*, ¶¶ 1 – 4).[2] Cohen brings his lawsuit on behalf of himself and all persons who "visited" the Retailer Websites and "had [their] electronic communications intercepted and disclosed to NaviStone" (*id.*, ¶¶ 3, 56). There is no allegation in the Amended Complaint explaining either how or in what respects Cohen or members of the proposed class suffered any pecuniary or other harm.

B. Navistone's Work on the Retailers' Behalf

Cohen alleges that the Retailers contracted with NaviStone to allow NaviStone to receive and analyze communications they receive as a result of visitors' interactions with their websites, all in an "attempt to learn his identity, postal address, and other PII ["personally identifiable information"]" for the purpose of sending him direct mail promotions (*id.* ¶¶ 1, 2, 16 (all the described activities occur pursuant to [the Retailers'] agreement with NaviStone"), 19 – 20). For purposes of Cohen's claims, the "electronic communications" at issue are expressly defined as follows:

> Plaintiff and Class Members' keystrokes, mouse clicks, and other interactions with [the Retailer Websites] are 'electronic communications' as defined by 18 U.S.C. § 2510(12).

(*id.* ¶ 47).

NaviStone, it is alleged, received these "electronic communications" because the Retailers added a "simple line of code" (provided by NaviStone) to their websites (the alleged "wiretap") (*id.* ¶¶ 11, 12). This code, according to Cohen, is "engaged as soon as the visitor arrives at" the websites, and the alleged interception commences immediately as a result of "loading the main page" of the websites (*id.* ¶ 22). Thus, "any information he may have typed

---

[2]This allegation of "scanning," new to the Amended Complaints, is among numerous false claims made by Cohen. NaviStone, similarly, has never captured the keystrokes of website visitors or sought to learn for itself—or reveal to its clients—their names and addresses. *See* NaviStone's Commitment to Consumer Privacy, https://www.navistone.com/consumer-privacy-0 (last visited February 20, 2018).

onto forms without clicking submit, or any keystrokes, mouse clicks or similar communications with [the Retailer Websites] ….", are transmitted, simultaneously, to NaviStone (*id.* ¶ 48). Upon receipt of this data, NaviStone analyzes it to determine which visitors are most likely to respond to a direct mail promotion and to obtain these visitors' mailing addresses for use in the Retailers' direct mail advertising efforts (*id.* ¶¶ 18 – 20).

These allegations are consistent with Cohen's original Complaints. However, he has modified the Amended Complaints in two ways.

First, Cohen states, on "information and belief," that the line of code (the alleged "wiretap") not only results in communications to NaviStone, but also searches visitors' computers and other web-browsing devices to look for "tracking files employed by other websites or online data brokers to de-anonymize and identify the users." (Am. Compl. ¶ 32). He offers no details as to how this happens, or any examples of its occurrence.

Second, Cohen alleges that "at least some" of his website interactions while visiting the Retailer Websites "were not communications to which [the Retailers] and NaviStone were intended to be parties," but, rather, were communications with his "Internet service provider" only "for the purpose of accessing web content" (*id.* ¶ 48), although all of the "electronic communications" at issue in Cohen's case are expressly defined as "interactions with [Retailer Websites] …." (*id.* ¶ 43). Cohen does not identify which interactions with the Retailer Websites may have been intended for his Internet service provider ("ISP") alone.

C. The Alleged Wrongdoing

The Amended Complaints, like the originals, accuse the Retailers and NaviStone of five violations of the Wiretap Act:

- **Count I** claims that § 2511(1)(a) has been violated by the "interception" of "electronic communications" in violation of the Wiretap Act (Am. Compl. ¶ 48);

- **Count II** claims that § 2511(1)(b) has been violated because Defendants wrongfully disclosed these "intercepted" communications to each other and to unidentified third parties (*id.* ¶ 50);

- **Count III** claims that § 2511(1)(d) has been violated because Defendants wrongfully used the contents of visitors' communications "to de-anonymize them, and for other purposes" (*id.* ¶ 52);

- **Count IV** claims that § 2511(1)(a) has been violated because Defendants "procuring" one another to engage in interception of interactions between website visitors" the Retailer Websites (*id.* ¶¶ 54-55); and

- **Count V** claims that § 2512 has been violated because Defendants manufactured, distributed, and possessed an "electronic, mechanical, or other device," as defined by 18 U.S.C. § 2510(5), for use in "surreptitious interception of electronic communications" (*id.* ¶¶ 57-59).

The Amended Complaints add three new claims:

- **Count VI** claims that the SCA has been violated by Defendants having "intentionally accessed stored files on Plaintiff's and Class members' computers and devices without authorization or by exceeding an authorization given" (*id.* ¶¶ 69-70); and

- **Count VII** claims that defendants have violated New York General Business Law § 349 because their "wiretapping" and "scan of the user's computers constitute "deceptive acts and practices."

- **Count VIII** claims that § 350 of the same law has been violated because the "wiretapping" and "scan of the user's computer" is "false advertising."

The Amended Complaints does not allege any defined injury to Cohen or any putative class members. It does claim, however, that Cohen and each class member are entitled to recover "any profits made by Defendants as a result of [alleged Wiretap Act] violations, statutory damages of whichever is greater of $100 a day for each day of violation or $10,000 for each class member," "statutory damages of $1,000" for alleged SCA violations, and "equitable or declaratory relief, punitive damages, and reasonable attorney's fees and litigation costs," as well as "restitution" *(id.,* "Wherefore" Cl. ¶¶ D, E, H). Statutory damages are also alleged under GBL §§ 349 and 350 (*id.* ¶ F).

ARGUMENT

I. Legal Standard to Be Applied

On a Rule 12(b)(6) motion to dismiss for failure to state a claim, "the factual allegations in a complaint are accepted as true and all reasonable inferences are drawn in the plaintiff's favor." *DigitAlb, Sh.a v. Setplex, LLC*, No. 17-CV-4102, 2018 WL 377381, at *2 (S.D.N.Y. Jan. 11, 2018) (citation omitted). As this Court has stated:

> To survive a motion to dismiss, the complaint "must contain sufficient factual matter" to "state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). In other words, the "[f]actual allegations must be enough to raise a right to relief above the speculative level." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). While a complaint "does not need detailed factual allegations" to survive a motion to dismiss, *Bell Atl. Corp.*, 550 U.S. at 555, 127 S.Ct. 1955, a pleading that merely recites conclusory allegations or a "formulaic recitation of the elements of a cause of action" fails to state a claim, *Iqbal*, 556 U.S. at 678.

Id. (citations omitted).

II. Cohen Fails to State a Claim under the Wiretap Act.

The Amended Complaints state repeatedly that the line of software code the Retailers obtained from NaviStone—installed by the Retailers on their own websites—implemented a "wiretap." According to Cohen, "[p]ursant to an agreement with Navistone," the Retailers "intentionally embedded NaviStone's coded wiretap" the Retailer Websites "to intercept visitors' communications to obtain de-anonymized PII" (Amend. Compl. ¶ 16). According to Cohen, "Plaintiff's and Class Members' keystrokes, mouse clicks, and other interactions with [the Retailer Websites] are 'electronic communications' as defined by 18 U.S.C. § 2510(12)" (*id.* ¶ 47). These allegations show that the activities described in the Complaint do not constitute unlawful wiretapping for three reasons.

A. NaviStone "Is a Party to the Communication" Under § 2511(2)(d).

The Wiretap Act imposes civil liability on any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" (§ 2511(1)(a)); uses a "device to intercept any oral communication" under specified circumstances (*id.* subdiv. (b)); discloses to others the contents of information knowingly "obtained through the interception of a wire, oral, or electronic communication" (*id.* subdiv. (c)); or intentionally uses information "obtained through the interception" of such a communication (*id.* subdiv. (d)).

All of these prohibitions, however, rest on the requirement that the "wiretapper" has wrongfully intercepted a communication between other parties. *See* § 2511(2)(d) (excluding from liability "a person . . . intercept[ing] a wire, oral, or electronic communication where such person is a party to the communication"). Thus, anyone who is a sender or a recipient "is a party to the communication" and not subject to the prohibitions of the Wiretap Act. *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125, 143 (3d Civ. 2015), *cert. denied sub nom.*, *Gourley v. Google, Inc.*, 137 S.Ct. 36 (2016).

At issue in this case are "electronic communications" that occur when visitors browse the Retailer's websites. According to the Amended Complaints, Retailers cause this data to be forwarded, in real time, to NaviStone. Accepted as true, these allegations thus establish that both Retailers and NaviStone are direct parties to "electronic communications" on which Amended Complaint rests. *See, e.g., In re DoubleClick Inc. Privacy Litigation,* 154 F.Supp.2d 497, 514 (S.D.N.Y. 2001).

The Third Circuit's ruling in *Google*, *supra*, is illustrative of the effect of § 2511(2)(d). In that case, the defendants were third-party advertising providers that placed "cookies" on a website user's device each time the user visited certain their clients' websites.

The cookies were codes issued by and through these websites that permitted tracking of the user's Internet activities. 806 F.3d at 133. As here, the *Google* plaintiffs' complaints conceded, as here, that the plaintiffs had intended to visit the websites from which the codes emanated, further alleging that "[u]pon receiving a … request from the user seeking to display a particular webpage, the server for that webpage will subsequently respond to the browser, instructing the browser to send a … request to the third-party company [Google] charged with serving the advertisements for that particular webpage." 806 F.3d at 140. The Third Circuit held that these allegations admitted that the website owners and their advertising providers were each a "party to the communication" under § 2511(2)(d) and therefore not in violation of the Wiretap Act. *Id.*

Here, Cohen alleges that when he visited the Retailer Websites, the alleged wiretap picked up "electronic communications" in the form of his "keystrokes, mouse clicks, and other interactions with [the Retailer Websites]" (Amend. Compl. ¶ 47). These communications were allegedly sent immediately to NaviStone because of the "NaviStone software coded wiretap" (*id.*, ¶ 16). NaviStone was thus, by Cohen's own allegations, a party to the communications described in the Complaint. This is the very result obtained in *Nickelodeon*, *supra*. There, the Third Circuit, applying *Google*, held that neither Viacom, the operator of certain websites, nor Google, violated the Wiretap Act by placing cookies on users' computers to track the activities of children on those websites. It was the parties that placed the cookies on the computing device that were the relevant "parties to the communications," meaning that they could not be held liable under the Wiretap Act. 827 F.3d at 275 (citing *Google*, 806 F.3d at 137).[3]

[3]As in his original Complaint, Cohen does not make clear whether the electronic communications are sent to NaviStone by the Retailers rather than directly by Cohen. Here, as there, this ambiguity is immaterial—under either characterization the legal result is the same, as

In his Amended Complaints, Cohen for the first time attempts to avoid dismissal by stating, in a single new paragraph, that "at least some" of the interactions he may have had with the Retailer Websites were intended to be communications *with his ISP alone*, not the Retailers or NaviStone. (Amend. Compl. ¶ 48). This bald statement of intention as to certain unidentified communications is at odds with every other pertinent allegation he makes concerning the nature of his communications. In the original Complaints, for example, Cohen could not have been clearer in stating the obvious: that the lawsuits were based on the fact that Defendants "wiretapped his communications *with the website*, …." (Orig. Compl. ¶ 2) (emphasis added). While he managed to delete these three words from ¶ 2 of the Amended Complaints, he retains this description when expressly identifying the "electronic communications" upon which his case rests: "Plaintiff's and Class Members' *keystrokes, mouse clicks, and other interactions with Casper.com [i.e., with the Retailer Websites]* are "electronic communications" as defined by 18 U.S.C. § 2510(12)" (Amend. Compl. ¶ 47). ("Other Allegations Common to All Claims")) (emphasis added).[4]

Cohen's claim of an intent solely to communicate with his ISP is also nonsensical. It is akin to a person claiming that, in calling a retailer's telephone number, it was his intention to

---

NaviStone is an authorized recipient of communications from Cohen, either as a party to the communication or as a result of the "prior consent" it received from the Retailers for *all* of its activities (*see* pp. 12-14 *infra*).

[4]If this was not clear enough, Cohen alleges that the communications took place "during each of Plaintiff's visits" to the Retailer Websites (Amend. Compl. ¶ 2); while "browsing" Retailer Websites (*id.* ¶¶ 1, 14); beginning "as soon as the visitor loads [the Retailer Websites] into their web browser" (*id.*); "as soon as the visitor arrives at [the Retailer Website]" (*id.* ¶ 22); occur "[a]s the visitor interacts with [the Retailer Websites]" (*id.* ¶ 23); "[w]hen [the Retailer Website] is loaded into a browser" (*id.* ¶ 26); "as he or she browses" the Retailer Websites (*id.* ¶ 33); and "[w]hen filling out forms" on the Retailer Websites (*id.* ¶ 34). In other words, all of the allegedly actionable communications occurred in connection with his browsing the Retailer Websites. Avoiding the words "Retailer Websites" does not obscure Cohen's meaning.

speak just with the phone company. *See, e.g., Mashatantucket Pequot Tribe v. Redican*, 309 F. Supp. 2d 309, 312 (D. Conn. 2004) ("Every web page has its own web site, which is its address, similar to a telephone number or street address."). As this Court explained in *In re DoubleClick Inc. Privacy Litigation*, *supra*, users, like Cohen, access web pages by sending requests to the servers that store those pages for their owners. 154 F.Supp.2d at 501. While an ISP gives the user access to the pipeline (the "vast collection of interconnected computer networks") over which digital data passes, the user's communication is addressed specifically to website's server, not the ISP. *Id.* In response to the user's request for access to a web page, and his interaction with that website, it is the hosting server (not the ISP) which receives and sends back the communications. *Id.*

As the Third Circuit observed in affirming the dismissal of a Wiretap Act claim in *Google*, the Court may dismiss a complaint "when [the] defendant's plausible alternative explanation" of the inferences to be drawn from the complaint "is so convincing that plaintiff's explanation is *im*plausible." *Google*, 806 F.3d at 142 & n.70 (brackets and emphasis in original; quotation and citations omitted). As in *Google*, Cohen cannot have it both ways, seeking to hold Defendants liable for intercepted content from visits to the Retailer Websites, while simultaneously claiming that he never intended to communicate with those websites when he visited them. The Retailers, in other words, could not cause to be forwarded to NaviStone information that was not communicated to them in the first instance, thus rendering Cohen's claim of ISP-only communications absurd.

B. NaviStone Does Not "Intercept" Any Electronic Communications.

These same allegations in Cohen's Amended Complaints negate another indispensable element of a Wiretap Act violation: namely, the occurrence of an "interception" of a communication between senders and recipients.

The statute, in § 2511(1), applies only to "any person who— (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." The Wiretap Act defines the word "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." § 2510(4). "Electronic communication" is defined in relevant part as "any transfer of signs, signals, writing, images," etc. § 2510(12).

The courts have held, therefore, that "intercept" means an "acquisition" of information "during the transfer, or during the course of transmission." *Fraser v. Nationwide Mutual Ins. Co.*, 135 F. Supp. 2d 623, 634 (E.D. Pa. 2001), *aff'd in relevant part,* 352 F.3d 107, 113 (3d Cir. 2003) ("an 'intercept' . . . must occur contemporaneously with transmission."); *see generally, United States v. Turk*, 526 F.2d 654 (5th Cir. 1976), *cert. denied* 429 U.S. 823 (1976).

From this definition of "intercept," it follows that the required element of interception can only occur between the sending and receipt of information. For an interception to occur, the intervener must have obtained access to the communication *before* it reached the recipient of that communication. *See In re Vizio, Inc. Consumer Privacy Litigation*, 238 F.Supp.3d 1204, 1228 (C.D. Cal. 2017) (dismissing Wiretap Act claim for failure to allege with sufficient clarity that defendant "intercepted their electronic communications 'during transmission'").

In this case, the Amended Complaints fail to demonstrate an actionable "interception." There is no allegation that either the Retailers or NaviStone availed themselves of information during transmission, only that the communications were sent to them by Cohen and analyzed after receipt. A recipient cannot, by definition, intercept a communication sent to it.

Because NaviStone, under its agreement with the Retailers, is a recipient of the communication, the acquisition of information does not occur "during transmission" from the sender, Cohen, but only when "transmission is complete." *See In re Facebook Internet Tracking Litigation* 263 F. Supp. 3d 836, 844-45 (N.D. Cal. 2017).

C. Navistone Had the Prior Consent of the Retailers, Each a Party to the Communications At Issue, for All of Its Activities.

For liability to attach to NaviStone under the Wiretap Act, the alleged "interception" of a communication must have been undertaken without the consent of at least one of the parties to that communication. *See In re DoubleClick Privacy Litigation*, 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001) (no liability under the Wiretap Act where DoubleClick-affiliated websites authorized DoubleClick's access). Indeed, the Wiretap Act explicitly provides that there is no unlawful interception where such consent exists. 18 U.S.C. § 2511(2)(d). *See, e.g., Vasko v. Twyford,* No. CV 16-197, 2016 WL 3522038 at *5 (W.D. Pa. June 28, 2016) (consent from one party "is a complete defense under the Wiretap Act"); *See Chance v. Ave. A, Inc.*, 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001) ("It is implicit in the web pages' code instructing the user's computer to contact Avenue A . . . that the web pages have consented to Avenue A's interception of the communication between them and the individual user."); *see also United States v. Amen*, 831 F.2d 373, 378 (2d Cir. 1987) ("Congress intended the consent requirement to be construed broadly.").

Here, the consent of the Retailers to all of NaviStone's activities is not only expressly stated by Cohen, but also infuses and informs every material allegation of the Amended Complaints. Cohen specifically alleges that all of NaviStone's activities were at the behest of the Retailers under a contractual relationship between them, one in which the Retailers themselves installed on their own website the software code alleged to constitute a "wiretap" for

purposes of forwarding information to NaviStone for analysis. As a result, NaviStone's activities did not violate, and could not have violated, the Wiretap Act. *See also In re Nickelodeon Consumer Privacy Litigation*, *supra*, 827 F.3d at 274-75; *In re Trilegiant Corporation, Inc.*, 2016 WL 8114194 *11, Civil Action No. 3:12-CV-0396 (D. Ct. Aug. 23, 2016); accord *Chance v. Ave. A, Inc.*, 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001).

This Court's decision in *In re DoubleClick Inc. Privacy Litigation*, 154 F.Supp.2d 497 (S.D.N.Y. 2001), is virtually on "all fours" with the case at bar. *DoubleClick*, like NaviStone, served as a third-party marketing company that entered into marketing partnerships with website owners. Under these contracts, and just as with NaviStone, communications between website visitors and the website owners were forwarded to DoubleClick, in real time. DoubleClick then analyzed these communications for the purpose of determining whether to send website visitors targeted online advertisements, *e.g.*, "banner advertisements," to which they were deemed likely to respond by DoubleClick. 154 F. Supp. 2d at 503-04. DoubleClick, like NaviStone, applied an algorithm to the information it obtained "to determine which advertisements it will present to the user." *Id.* at 503. The communications from website visitors directed to DoubleClick included the same information alleged to be transmitted to NaviStone, including "query strings" (showing pages and items visited by a user); form-field information ("when they fill-in multiple blank fields on a webpage," including names, addresses, and email addresses); and data concerning "the users' movements throughout the affiliated Web site, enabling DoubleClick to learn what information the user sought and viewed" *id.* at 504. The complaint also alleged that the DoubleClick "aggregates and compiles [this] information to build demographic profiles of users," and targets banner advertisements "using these demographic profiles." *Id.*

In *DoubleClick*, the Court found that the client websites "are 'parties to the communication[s]' from plaintiffs," and, equally important, these website owners "have given sufficient consent to DoubleClick to intercept them." *Id.* at 514. Accordingly, neither DoubleClick, nor its website-owning clients, could be liable under the Wiretap Act. So, too, is it here because NaviStone admittedly had the "prior consent" of the Retailers to all of its activities. *Id.* at 510 ("[The Wiretap Act] in no way outlaws collecting personally identifiable information or placing cookies, qua such. All that the Web sites must authorize is that DoubleClick access plaintiffs' communications to them.").

In the appropriate case, liability may attach even in the case of consent where the "primary motivation" or a "determinative factor" for an interception is to commit a criminal or tortious act. *Nickelodeon,* supra, 827 F.3d at 275. However, the tortious act exception must be "narrowly construed," *DoubleClick*, *supra*, 154 F.Supp. at 515, and "only applies when the offender intercepted the communication for the purpose of a tortious or criminal act that is *independent* of the intentional act of recording." *Nickelodeon*, 827 F.3d. at 276 (emphasis in original). Here, the Complaint affirmatively pleads on its face the absence of such an *independent* tortious or criminal purpose, stating instead that NaviStone's partnership with the Retailers was for the purpose of developing a list of mailing addresses for direct mail promotions (Compl. ¶¶ 1, 14, 18).

It is anticipated that Cohen may argue that the question of "prior consent" is a statutory exception, not an element of his claim, that ought not be addressed on a motion to dismiss. It is well-established, however, that courts "may dismiss a claim based on a statutory exception that appears on the face of the complaint." *DoubleClick*, 154 F. Supp. 2d at 507. As the district court in *DoubleClick* explained:

> Thus, if DoubleClick's conduct falls into one of § 2701(c)'s exceptions on the face of the complaint, it is proper for us to dismiss the claim as one within a statutory exception. Furthermore, even if § 2701(c) was construed as an affirmative defense, the Second Circuit has held that a court may properly dismiss a claim on the pleadings when an affirmative defense appears on its face. *See Day v. Moscow*, 955 F.2d 807, 811 (2d Cir. 1992) ('[W]hen all relevant facts are shown by the court's own records, of which the court takes notice, the [affirmative] defense may be upheld on a Rule 12(b)(6) motion without requiring an answer'); *see generally* 2 James Wm. Moore et al., *Moore's Federal Practice* § 12.34[4][b] (3d ed. 2000).

Id. at 508.

III. Count V Should Be Dismissed: No Private Cause Of Action Exists under 18 U.S.C. § 2512 and the Requisite "Device" Is Not Specifically Identified.

Besides the foregoing, there are separate and independent grounds for dismissing Count V, which alleges that NaviStone intentionally created "wiretaps" or "wiretap codes," possessed them, advertised them, and distributed them for installation in violation of 18 U.S.C. § 2512(1)(b) (Compl. ¶¶ 56 – 59).

This claim has two fatal problems. First, there is no private right of action under 18 U.S.C. § 2512. Second, even if there were, the Amended Complaints do not identify any actual "electronic, mechanical, or other device," a necessary element of any such hypothetical claim. *See* 18 U.S.C. § 2510(5). The Complaints attempt to confuse the issue by referring freely to "wiretaps" or "wiretap codes," as if those were established "devices." They are not. Section 2512(1)(b) of Title 18 of the United States Code provides, in pertinent part, that it is unlawful to

> manufacture[], assemble[], possess[], or sell[] *any electronic, mechanical, or other device*, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications …

Id. (emphasis added).

The clear weight of authority is that no private cause of action is available under Section 2512(1)(b). "[A]s a matter of grammar and sentence structure," the Wiretap Act

provides a cause of action for "interception, disclosure, or intentional use of communications," not the "possession of prohibited devices." *DirecTV, Inc. v. Bertram*, 296 F. Supp. 2d 1021, 1024 (D. Minn. 2003); *see also DIRECTV, Inc. v. Cignarella*, 2005 WL 1252261, at *3 *(D.N.J. May 24, 2005)* (rejecting a Section 2512 private right of action and holding that "in order to be civilly liable, a defendant must have intercepted, disclosed or intentionally used a plaintiff's wire, oral or electronic communications"); *DIRECTV, Inc. v. Robson*, 420 F.3d 532, 539 (5th Cir. 2005) (same); *DirectTV v. Treworgy*, 373 F.3d 1124, 1128-29 (11th Cir. 2004) (same); *see also DIRECTV, Inc. v Pepe*, 431 F.3d 162, 166 n.8 (3d Cir. 2005) (sustaining dismissal of Section 2512 claims not raised on appeal).

Moreover, the Amended Complaints appear to equate alleging the insertion of "a small parcel of computer code" on the Retailers' website with alleging the existence of a "device." But for all their discussion of how the code works, the Amended Complaints never identify any object that itself could constitute the "device or apparatus" required by § 2512. Absent such an allegation, the Cohen's Section 2512 claim must fail, even if a private cause of action upon which to bring such a claim were permitted.

IV. Cohen Fails to State a Claim under the Stored Communications Act.

The Amended Complaints also purport to assert a claim for relief under the SCA, 18 U.S.C. § 2701, alleging (without any further explanation) that Defendants "scanned" or "searched" his computer for "tracking files employed by other websites or online data brokers" in order to de-anonymize and identify him. The Court should disregard this "naked assertion." *See Santiago v. Warminster* Twp., 629 F.3d 121, 131 (3d Cir. 2010) (citing *Ashcroft v. Iqbal*, 556 U.S. 662 (2009)). Plaintiff did not include this allegation in his original complaints and, presumably because it has no basis in truth, he offers no elaboration or factual development in

his Amended Complaint sufficient to give NaviStone "fair notice of what the ... claim is and the grounds upon which it rests." *Conley v. Gibson*, 355 U.S. 41, 47 (1957).

Even if Cohen's claims were given any credence at all, to state an SCA claim, a plaintiff must show that the defendant (1) intentionally accessed without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeded an authorization to access such a facility. *Id.* at 145–46 (quoting 18 U.S.C. § 2701(a)). Here, Cohen's entire SCA claim is predicated on the defendants allegedly scanning and accessing files on visitors' personal web-browsing devices. (Amend. Compl. ¶ 74 ("Plaintiff's and Class members' computers and devices are facilities through which an electronic communications service is provided."). Such devices, however, do not constitute the type of service-providing facility that is protected by the SCA. *See, e.g., In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d at 511 ("Clearly, the cookies' residence on plaintiffs' computers does not fall into § 2510(17)(B) because plaintiffs are not "electronic communication service" providers."); *See also Nickelodeon*, 827 F.3d at 276–77 (same); *Google*, 806 F.3d at 145 (same); accord *Cousineau v. Microsoft Corp.*, 6 F. Supp. 3d 1167, 1174–75 (W.D. Wash. 2014) (agreeing that the "overwhelming body of law" supports the conclusion that a personal computer or other device is not a "facility" for purposes of liability under the SCA) (citations and quotations omitted).

Further, even if personal devices somehow qualified as a "facility that provides electronic communications service," the Amended Complaints do not allege access to any "communications." Specifically, Cohen avers that his computer was scanned by NaviStone for "tracking files employed by other website or online data brokers," not for communications between Cohen and any other parties. Nor are such files in "electronic storage" for purposes of the SCA. As the Fifth Circuit has explained, electronic storage "encompasses only the electronic

information that has been stored by an electronic communication service provider." *Garcia v. City of Laredo,* 702 F.3d 788, 793 (5th Cir. 2012). Moreover, such information must be stored by the service provider either "temporarily pending delivery or for backup protection … But information than individual stores on his hard drive or cell phone is not in electronic storage under the statute." *Id.* (citations omitted). Because the tracking codes Cohen complains about are not stored by an electronic communication service provider either incident to transmission or for back up purposes, the Amended Complaints fail to assert a valid claim under the SCA.

V. The New State-Law Claims Should Be Dismissed.

Plaintiff has added two state law claims under New York's General Business Law ("GBL"), a claim for "deceptive acts or practices" under GBL § 349 (Count VII), and a claim for "false advertising" under GBL § 350 (Count VIII). In each Amended Complaint, Plaintiff alleges that NaviStone violated § 349 "by wiretapping visitors" to the retailer defendant's website and by using the website "to scan the user's computer in search of files that can be used to de-anonymize and identify the user" (Am. Compl. ¶ 66). The same alleged conduct is said to violate § 350 by being "misleading in a material way" (*id.* ¶ 72).

Neither Count is viable, and both should be dismissed, not just as a matter of the Court's discretion under the supplemental jurisdiction provisions of 28 U.S.C.§ 1367(c), but with prejudice because the claims have no merit on their face. Neither Count alleges an injury-in-fact, which is a requirement both for Article III standing and an element of a private cause of action under both statutory provisions. Neither Count can stand alone without the federal claims because both are premised on violations of these federal statutes. And neither Count alleges the kind of actively deceptive activity the two New York provisions were designed to prevent—indeed, no conduct that could have misled Plaintiff is alleged against NaviStone at all.

A. The State-Law Counts Fail to State a Claim.

Section 349 of the General Business Law makes it unlawful to engage in "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service" in New York. Section 350 makes it unlawful to engage in "[f]alse advertising" in the same context. A private right of action is available under GBL § 349(h) to "any person who has been injured by reason of any violation of this section". A private action is also permitted under § 350 for a "consumer who falls victim to misrepresentations made by a seller of consumer goods through false or misleading advertising." *Solomon v. Bell Atlantic Corp.*, 9 A.D.3d 49, 52, 777 N.Y.S.2d 50, 54 (1st Dep't 2004), quoting *Small v. Lorillard Tobacco Co.*, 94 N.Y.2d 43, 55, 698 N.Y.S.2d 615, 620 (1999). Three elements must be shown: (1) consumer-oriented conduct, (2) that is materially deceptive, and (3) *causes injury* to the plaintiff. *Shou Fong Tam v. Metropolitan Life Ins. Co.*, 79 A.D.3d 484, 486, 913 N.Y.S.2d 183, 185 (1st Dep't 2010).

No Injury. Neither Count VII nor Count VIII alleges the requisite injury. The New York Court of Appeals has made clear that simply being deceived cannot itself constitute a cognizable injury. *Small*, *supra*, 94 N.Y.2d at 56. The plaintiff must allege "a "manifestation of either pecuniary or 'actual' harm." *Id.* Unlike a private claim under the Wiretap Act or the SCA, the mere occurrence of the prohibited act under §§ 349 or 350 does not ipso facto create a presumption of injury. While one may infer that Cohen does not wish to be identified as having initiated contact with the retailers' websites, he makes no allegation of any "loss or detriment" to his property or person. B. Garner (ed.), *Black's Law Dictionary*, "harm", at 722 (7th ed. 1999). This failure to plead injury-in-fact warrants dismissal of both Counts for lack of Article III standing. *Spiro v. Healthport Technologies, LLC*, 73 F. Supp. 3D 259, 266-67 (S.D.N.Y. 2014).

It also warrants dismissal for failure to show an essential element of the state law causes of action. *Small*, *supra.*

No Federal Statutory Basis. Counts VII and VIII cannot survive as stand-alone claims if the Wiretap Act and the SCA claims are dismissed. Both Counts expressly presuppose the occurrence of alleged "wiretapping" and of a "scan of the user's computer," wrongs that are defined and made illegal in 18 U.S.C. § 2511 and § 2701 respectively. In contrast, GBL §§ 349 and 350 do not independently create liability for "wiretapping" or for making a "scan" of computers. They address "deceptive acts" and "false advertising." Without bolstering from the federal claims, the state-law counts do not, and cannot, show that either a "wiretap" or a "scan" amounts to a "deceptive act" or "false advertising." Dismissal of the Wiretap Act and SCA would mean that no predicate remains for any finding of wrongful conduct under state law. Thus, if the federal statutory claims are dismissed, the state-law claims must be dismissed as well. *See Broder v. Cablevision Systems Corp.*, 329 F. Supp.2d 551, 559 (S.D.N.Y. 2004), *aff'd*, 418 F.3d 187 (2d Cir. 2005).

No Deception. The state-law Counts also fail because they do not, and cannot, allege deception, which is an essential element of a private cause of action under both §§ 349 and 350. Indeed, it is mystifying that Plaintiff would invoke these provisions against NaviStone. Plaintiff's pleading repeatedly accuses NaviStone of stealth, of hiding its use of codes "through dummy domains to attempt to conceal its activities" (Am. Compl. ¶ 17). This is the opposite of the kind of affirmative misstatements or omissions of material facts that §§ 349 and 350 are intended to prohibit.

The legislative purpose of these provisions is to preserve "an honest marketplace where trust prevails between buyer and seller." *Oswego Laborers' Local 214 Pension Fund v.*

Marine Midland Bank, N.A., 85 N.Y.2d 20, 25 (1995), quoting Mem. Of Gov. Rockefeller, 1970 N.Y. Legis. Ann., at 472. This presupposes outreach by commercial parties to consumers. As Chief Judge Kaye states in *Oswego*, the law contains "an objective definition of deceptive acts and practices, whether representations or omissions, limited to those likely to mislead a reasonable consumer acting reasonably under the circumstances." 85 N.Y.2d at 26. The consumer must have acted in response to something affirmative from the commercial party that the consumer was misled by while acting reasonably under the circumstances. Whether the claim is valid "may be determined as a matter of law or fact (as individual cases require)". *Id.*

Given this legislative intent, Cohen does not allege deception of the kind required for a claim under §§ 349 or 350. There has been no outreach by NaviStone "likely to mislead a reasonable consumer acting reasonably under the circumstances." No active misrepresentation is alleged nor is any material fact claimed to have been omitted from any message, transmittal, or advertisement directed by NaviStone to consumers in general or to Plaintiff in particular, because NaviStone is not alleged to issue such communications. Indeed, Cohen apparently only learned NaviStone even existed by reading two *Gizmodo* online articles (Amend. Compl. ¶¶ 18, 21).

In short, the absence of any allegations of deception that go beyond the conduct alleged to have violated federal law destroys the state-law Counts as stand-alone claims. *Broder*, *supra*, 329 F. Supp.2d at 559 (dismissing § 349 claim where complaint was "devoid of any allegations of deception beyond the violations of" federal law); *see also Fink v. Time Warner Cable*, 837 F. Supp. 2d 279, 284 (S.D.N.Y. 2011), *aff'd*, 714 F.3d 739 (2d Cir. 2013).

B. The State-Law Claims Should Be Dismissed under 28 U.S.C. § 1367(c).

The Court "may decline to exercise supplemental jurisdiction… if— … (3) the district court has dismissed all claims over which it has original jurisdiction". 28 U.S.C. § 1367(c)(3). *Arbaugh v. Y&H Corp.,* 546 U.S. 500, 514 (2006). While district courts in their discretion may continue to hear state-law claims even if the federal claims have been dismissed, ordinarily they will not exercise that discretion unless a statute of limitations has run or substantial progress has already been made in the proceedings. *See, e.g., RWJ Mgmt. Co. Inc. v. BP Products North America, Inc.*, 672 F.3d 476, 479 (7th Cir. 2012). Neither exception exists in the present case; supplemental jurisdiction should be declined.

CONCLUSION

As in the case of *DoubleClick*, decided by this Court in 2001, Cohen's' Amended Complaints fail to present actionable violations of any of the statutes under which he brings suit. As the Court in *DoubleClick* explained:

> "[t]he absence of evidence in the legislative or judicial history of any of these Acts to suggest that Congress intended to prohibit conduct like DoubleClick's supports this conclusion. To the contrary, the histories of these statutes reveal specific Congressional goals-punishing destructive hacking, preventing wiretapping for criminal or tortious purposes, securing the operations of electronic communication service providers-that are carefully embodied in these criminal statutes and their corresponding civil rights of action.

154 F. Supp. 2d at 526. The same is true for NaviStone and the Retailers, whose described activities are identical in all material respects to those considered in DoubleClick. The Internet-based advertising described in the Amended Complaints falls outside both the express terms of the federal laws Cohen invokes and their legislative purposes. By their own terms, the Amended Complaints allege conduct by NaviStone that constitutes perfectly lawful, appropriate and socially beneficial activity.

For all the reasons stated above, and upon a careful review of the pleading itself, the Amended Complaints should be dismissed as a matter of law.

Dated: New York, New York
March 1, 2018

Respectfully submitted,

MENAKER & HERRMANN LLP

By: Richard G. Menaker
Richard G. Menaker

10 East 40th Street
New York, New York 10016
Attorneys for Defendant NaviStone, Inc.

BRANN & ISAACSON
David W. Bertoni, *Pro hac vice*
184 Main Street, P.O. 3070
Lewiston, Maine 04243-3070
Of Counsel.